BRIAN M. LUTZ, SBN 255976
blutz@gibsondunn.com
WESLEY SZE, SBN 306715
wsze@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200

JASON J. MENDRO, SBN 220842
jmendro@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500

*Attorneys for Defendants*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO DIVISION**

IN RE OKTA, INC. SECURITIES LITIGATION

CASE NO. 3:22-cv-02990-SI

**DEFENDANTS' NOTICE OF MOTION AND MOTION TO DISMISS AMENDED COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF**

*[Request for Judicial Notice; Declaration of Brian M. Lutz and Exhibits 1 to 9 attached thereto; and [Proposed] Order filed concurrently]*

**HEARING:**
Date: March 17, 2023
Time: 10:00 a.m.
Judge: Hon. Susan Illston
Courtroom: 1, 17th Floor

**TO THE COURT, ALL PARTIES, AND THEIR ATTORNEYS OF RECORD:**

**PLEASE TAKE NOTICE** that on March 17, 2023, at 10:00 a.m., or as thereafter as the matter may be heard before the Honorable Susan Illston, in Courtroom 1, Seventeenth Floor, of the United States District Court for the Northern District of California at 450 Golden Gate Avenue, San Francisco, CA 94102, Defendants Okta, Inc., Todd McKinnon, Brett Tighe, and Frederic Kerrest will, and hereby do, move this Court, pursuant to Rules 9(b), and 12(b)(6) of the Federal Rules of Civil Procedure, for an order dismissing the Amended Complaint. The Amended Complaint fails to plead particularized facts, as required under the Private Securities Litigation Reform Act of 1995 ("PSLRA") or Rule 9(b) of the Federal Rules of Civil Procedure, demonstrating that any defendant made a false or misleading statement or acted with scienter when making any challenged statement.

Defendants' motion is based on this notice of motion and motion, the accompanying memorandum of points and authorities, the accompanying request for judicial notice, the declaration of Brian M. Lutz and Exhibits 1 to 9 attached thereto, and any other documents on file in this action and any oral argument of counsel.

Dated: December 1, 2022

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Brian M. Lutz*
Brian M. Lutz

*Attorneys for Defendants Okta, Inc., Todd McKinnon, Brett Tighe, and Frederic Kerrest*

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

Page(s)

**Cases**

**Statutes**



**Regulations**

## MEMORANDUM OF POINTS AND AUTHORITIES

## I. PRELIMINARY STATEMENT

This is the latest in a recent spate of meritless lawsuits that attempt to transform unanticipated cyberattacks into securities fraud claims against the victims of those attacks. These suits rest on formulaic assertions that a company should have disclosed an incident faster and publicly declared its security vulnerabilities, and that warning investors about the risk of a security incident amounts to securities fraud when one had already occurred. This lawsuit should be the next in a long line of these misguided cases that have been dismissed.

This lawsuit arose from news in March 2022 that a hacker had gained access to an Okta vendor's computer and posted screenshots captured during the intrusion. Okta promptly reported everything it knew about the intrusion—that Okta had identified the suspicious activity and blocked the compromised account, and the hacker never breached Okta's systems and accessed no sensitive information about Okta's customers. Okta later reported that the incident had no quantifiable impact on Okta's financial results.

Litigants reflexively sued Okta, assailing the Company for not disclosing the incident sooner or condemning its own security measures. Although its themes are well worn, Plaintiff faced particularly unfavorable facts because the security incident at the heart of this case never even breached Okta's or its customers' systems, caused minimal harm, and was broadly disclosed soon after Okta learned about it.

Unhappy with the frail fraud claim it could craft from the security incident, Plaintiff pivoted to devise a completely different theory: that Okta lied about its integration of Auth0, a company it recently acquired. Despite Okta's repeated warnings that it may not be able to successfully operate as a combined company and that more work was required to integrate the Auth0 sales team, Plaintiff claims investors were misled by general, optimistic statements—"we're off to a fantastic start," "we're making great progress on the integration," and "we've made a lot of progress as a combined company." These and similar statements, Plaintiff contends, were shown to be fraudulent when Okta announced slower than anticipated growth earlier this year, as if the Company's optimistic updates and warnings promised investors that it would never face setbacks.

Both of Plaintiff's theories fail for two reasons. First, the Complaint is devoid of particularized factual allegations required under the Private Securities Litigation Reform Act of 1995 ("PSLRA") and Rule 9(b) to plead a material misstatement. Second, the Complaint fails to plead that Defendants acted culpably (i.e., with scienter) in any communication with investors.

**The Complaint Fails to Plead a Material Misstatement.** The Complaint alleges that general statements, like safety is "mission critical" to Okta, were false or misleading in light of the security incident, but these are classic puffery statements that are not capable of objective verification and cannot give rise to a securities fraud claim. Plaintiff also claims that Okta's risk factor warning investors about the possibility of security breaches was misleading because that risk had already materialized as a result of the security incident, but Plaintiff fails to plead that any material risk *had* materialized at the time of the warning or that Okta violated any duty by not disclosing earlier what it knew about the incident.

With respect to Plaintiff's Auth0 integration theory, virtually all of the challenged statements are general statements expressing optimism about the acquisition and the progress of the integration. These are textbook examples of non-actionable puffery. More fundamentally, Plaintiff ignores what Okta and its senior officers actually said about the challenges of integrating Auth0 into the Okta organization. In the same public filings and earnings call transcripts from which Plaintiff plucks snippets of inactionable puffery, Okta repeatedly warned investors that Okta may not be able to successfully integrate the Auth0 business, that key Auth0 employees may not stay with the combined company, and that Okta may struggle to retain Auth0 customers and business. Okta described its integration plan, including with respect to the sales team, and acknowledged that it was a work in progress. The Complaint misleadingly omits this important context and focuses on only the few words that fit Plaintiff's false narrative that Okta withheld from investors challenges with the integration strategy. Thus, even if the puffery statements could give rise to a claim under the federal securities laws—and they do not—there are no specific facts pleaded demonstrating that the statements, when read in full and in context, were materially false or misleading.

**The Complaint Fails to Plead Scienter.** The Complaint also should be dismissed on the separate ground that Plaintiff fails to plead particularized facts giving rise to a strong inference that any

Defendant knew or was deliberately reckless in not knowing that their statements were false or misleading. The Complaint pleads no facts demonstrating that any of the Individual Defendants were aware of information demonstrating that their public statements about Okta's commitment to security, the risks of a security breach, or the Auth0 integration were false or misleading. None of the confidential witnesses referenced in the Complaint claim to have first-hand knowledge of any information provided to or known by the Individual Defendants—let alone information demonstrating that they believed any challenged statement was untrue. At most, the Complaint claims that some of these witnesses believed that Okta's plan for integrating the sales teams faced setbacks due to employee attrition and difficulties in cross-selling Okta and Auth0 products. These opinions track the same warnings Okta provided to investors, and do not show the Individual Defendants knew or deliberately ignored that their general statements about Okta's "progress as a combined company," or that there was "still a lot of work to do," were false or misleading.

Nor is this one of the "exceedingly rare" cases where the nature of the alleged omissions concerning the security incident and the Auth0 sales integration were of "such prominence that it would be 'absurd' to suggest" that the Individual Defendants did not know their challenged statements were false or misleading. *S. Ferry LP, No. 2 v. Killinger*, 542 F.3d 776, 785 n.3, 786 (9th Cir. 2008) (internal citation omitted). The general nature of the statements themselves—Okta's commitment to security, a generic risk factor about security breaches, and that Okta was pleased with the integration but still had work to do with the sales team—also undercut Plaintiff's contention that the Individual Defendants must have known they were misleading to investors.

For all these reasons, the Complaint should be dismissed on the independent grounds that it fails to meet the heightened standard for pleading a material misstatement and scienter.

## II. STATEMENT OF THE ISSUES TO BE DECIDED

1. Whether Plaintiff's claim under Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 10b-5 should be dismissed for failure to plead that (a) any challenged statement was false or misleading at the time it was made; and (b) any Defendant acted with scienter.

2. Whether Plaintiff's claim under Section 20(a) of the Exchange Act should be dismissed for failure to plead a primary violation of the Exchange Act.

## III. BACKGROUND FACTS[1]

Okta, Inc. is the leading independent identity provider. (¶¶ 2, 214.) The Okta Identity Cloud provides identity and access management software that helps businesses securely connect their employees, contractors, and business partners to the right technologies at the right time. (¶ 2.) In 2009, Defendant Todd McKinnon, Okta's Chief Executive Officer, cofounded Okta with Defendant Frederic Kerrest, Okta's Chief Operating Officer. (¶¶ 32, 34.) Defendant Brett Tighe is Okta's Chief Financial Officer. (¶ 33.)

### A. Okta's Acquisition of Auth0

On March 3, 2021, Okta announced that it had entered into an agreement to acquire Auth0, a leading identity management platform for application developers, for $6.5 billion. (¶ 58.) The acquisition of Auth0 provided Okta with an opportunity to expand further into the identity market by offering a new product focused on identity management for a company's *customers*, which would complement Okta's focus on identity management for a company's *workforce*. (¶ 5; *see also id.* ¶ 59.)

Okta disclosed to investors the risks associated with combining the two companies. For example, in its press release announcing the completion of the transaction, Okta warned investors about "the ability of Okta and Auth0 to successfully integrate their respective businesses, . . . the loss of any Auth0 customers, the ability to coordinate strategy and resources between Okta and Auth0, and the ability of Okta and Auth0 to retain and motivate key employees of Auth0." (Ex. 1 at 4 (cited at ¶ 61).) In its quarterly financial report following the transaction, Okta also included risk-factor disclosures specifically related to the Auth0 acquisition, warning investors that "[a]ny integration process may require significant time and resources," and that Okta "may not be able to manage the [integration] process successfully as our ability to acquire and integrate larger or more complex companies, products, or technologies in a successful manner is unproven." (Ex. 2 at 9 (cited at ¶ 138).) Okta further cautioned investors that "there can be no assurances that our businesses can be combined in a manner

[1] By summarizing Plaintiff's allegations, Defendants do not concede that the allegations are true. Citations in the form of "¶ _" or "¶¶ _" refer to the paragraphs of the Amended Complaint (Dkt. 48). Citations to "Ex." refer to the exhibits to the Declaration of Brian M. Lutz, filed concurrently herewith, with pincites corresponding to the ECF pagination. As discussed in the accompanying Request for Judicial Notice, all of the exhibits are judicially noticeable and/or incorporated by reference in the Complaint.

that allows for the achievement of substantial benefits"—including because "it is possible that there could be a loss of [Okta's] and/or Auth0's key employees and customers." (*Id.*; *see also id.* at 10 ("We may incur significant, non-recurring costs in connection with the Acquisition and integrating the operations of Okta and Auth0, including costs to maintain employee morale and to retain key employees.").)

Following the completion of the acquisition in May, the "integration process began as promising." (¶ 78.) During Okta's September 2021 earnings call, McKinnon explained Okta's plan was to integrate the Auth0 and Okta sales teams by February 2022, which would "allow the unified sales team to sell both platforms and [would] benefit[] customers by providing more options to meet their unique use cases." (¶ 73.) He noted, however, that the Company still had "a lot more work to do at the detail level" (*id.*), and acknowledged that Okta "didn't have all the answers" with respect to the sales integration (¶ 74).

Over the next few months, Okta fine-tuned its integration strategy. In late 2021 and early 2022, the Company transitioned Auth0 salespeople from "specialists" (who focused only on selling Auth0 products) to "generalists" (who could sell the Company's full range of products). (¶¶ 81–83.) During a December 2021 earnings call, Kerrest explained: "We do have a lot on our plate," and the integration of the sales team is a "key piece of the puzzle." (¶ 85.) He added that the sales teams could not be combined with a "flip [of] the switch," and that the Company was "doing a lot of work . . . around education, [and] getting all the new folks ramped on now the broader suite of products that they're going to have to offer." (*Id.*)

Even after the Auth0 and Okta sales teams were unified in February 2022, as planned, Okta again "recognize[d] [that] there is still a lot of work to do." (¶ 93.) Tighe noted during a March 2022 earnings call that, despite Okta having more capacity for potential sales as a result of the combined sales teams, there were still "more pieces we need to finish up . . . [to] mak[e] sure that we're working as one organization going forward." (¶¶ 94–95.)

Okta reported "mixed" financial results in its second quarter of fiscal year 2023. (¶ 126.) As explained during its August 31, 2022 earnings call, the Company continued during the quarter to focus on integrating the Okta and Auth0 sales teams. *Id.* Even though they were continuing to "mak[e]

progress" with the ongoing integration efforts, "heightened attrition" and "some confusion in the field" had "impacted [Okta's] business momentum." (*Id.*) "Given [the] near-term outlook [and] the uncertainties of the macro environment," Okta would re-evaluate its financial targets for fiscal year 2026. (¶ 129.)

**B. The January 2022 Security Incident**

"In late January 2022, Okta detected an attempt to compromise the account of a third-party customer support engineer working for one of [Okta's] sub-processors." (¶ 106.) These engineers work for third parties retained by Okta and can "facilitate the resetting of passwords and multi-factor authentication factors" for Okta customers. (Ex. 6 at 4 (cited at ¶ 111).) As Okta explained in a blog post and webpage quoted throughout the Complaint (*see, e.g.*, ¶¶ 108, 111), as soon as Okta detected the unusual activity in January 2022, Okta "alerted the [third-party] provider to the situation, while simultaneously terminating the user's active Okta sessions and suspending the individual's account." (Ex. 5 at 2 (cited at ¶¶ 108, 186).) This was the only "evidence of suspicious activity in Okta systems." (Ex. 6 at 3.) "The matter was investigated and contained by the sub-processor." (Ex. 5 at 3.)

On March 21, 2022, a hacking group posted screenshots of Okta's platform on social media, which had been taken when the threat actor gained access to the sub-processor employee's computer in January 2022. (¶ 105.) McKinnon and Okta promptly confirmed (via Twitter and a blog post on March 22) that Okta was aware of this incident (¶¶ 106, 108), and that the Company was "actively continuing [its] investigation" (Ex. 5 at 3). Okta notified all customers whose profiles were *potentially* accessible from the sub-processor's employee's computer, which Okta estimated to be up to 2.5% of Okta customer base—an amount Okta acknowledged was likely "overinclusive"—even as the Company continued to investigate the incident. (Ex. 6 at 5; ¶¶ 108, 187.) Because the threat actor's access was restricted to the limited information the compromised Support Engineer could access on their computer, the threat actor never breached Okta's systems and never accessed customer databases. (Ex. 6 at 4.)

Despite the limited nature of the security incident and its minimal impact on Okta customers, Okta took responsibility for the events. In a webpage Plaintiff cites in the Complaint, Okta stated as follows:

> We want to acknowledge we made a mistake. Sitel [the compromised third-party sub-processor] is our service provider for which we are ultimately responsible.
>
> In January [2022], we did not know the extent of the Sitel issue – only that we detected and prevented an account takeover attempt and that Sitel had retained a third party forensic firm to investigate. At that time, we didn't recognize there was a risk to Okta and our customers. We should have more actively and forcefully compelled this information from Sitel.

(Ex. 6 at 3–4.)[2]

During Okta's next two quarterly earnings calls, Okta reported that the security incident had no "quantifiable impact" on Okta's financial results. (Ex. 8 at 4 (quoted at ¶¶ 162–63); Ex. 9 at 4 (quoted at ¶¶ 20, 126–29, 194–97).)

## IV. LEGAL STANDARD

To state a Section 10(b) claim, a complaint must allege facts sufficient to establish that (1) a material misrepresentation or omission; (2) was made with scienter ("a wrongful state of mind"); (3) in connection with the purchase or sale of a security; (4) on which plaintiff relied; (5) economic loss; and (6) loss causation. *Loos v. Immersion Corp.*, 762 F.3d 880, 886–87 (9th Cir. 2014). "[P]laintiffs in private securities fraud class actions face formidable pleading requirements to properly state a claim and avoid dismissal under [Rule] 12(b)(6)." *Metzler Inv. GMBH v. Corinthian Colleges, Inc.*, 540 F.3d 1049, 1054–55 (9th Cir. 2008). Plaintiffs must satisfy the "dual pleading" requirements of both the PSLRA and Federal Rule of Civil Procedure 9(b). *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 990 (9th Cir. 2009). "Rule 9(b) requires particularized allegations of the circumstances constituting fraud, including identifying the statements at issue and setting forth what is false or misleading about the statement and why the statements were false or misleading at the time they were made." *In re Rigel Pharms., Inc. Sec. Litig.*, 697 F.3d 869, 876 (9th Cir. 2012). And the PSLRA is even stricter: to "deter non-meritorious lawsuits," Congress enacted the PSLRA to "creat[e] procedural barriers such as heightened pleading standards." *In re LifeLock, Inc. Sec. Litig.*, 690 F. App'x 947, 950 (9th Cir. 2017) (citation omitted). The PSLRA further "requir[es] plaintiffs to state with particularity

[2] In April 2022, Okta disclosed findings from its further investigation in a current report on Form 8-K (filed voluntarily under Item 8.01), which confirmed that the security incident was even more limited than the "worst case scenario" impact Okta had disclosed the prior month (*see* Ex. 7 at 3). Okta reported that the threat actor had gained access to support engineer's computer for 25 minutes and only viewed non-sensitive information belonging to just two customers. (*Id.*) The Complaint does not plead any allegations disputing the accuracy of the statements that Okta disclosed through this Form 8-K.

both the facts constituting the alleged violation and the facts evidencing scienter." *Rigel*, 697 F.3d at 876. "These heightened pleading requirements . . . present no small hurdle," *Macomb Cty. Emps.' Ret. Sys. v. Align Tech., Inc.*, 39 F.4th 1092, 1096 (9th Cir. 2022) (internal quotations and citation omitted), which the Complaint fails to clear.

## V. ARGUMENT

This is an opportunistic suit that tries to capitalize on criminal activity that victimized Okta and its customers. This is not the first of its kind. Other cases like this one have been filed in California and nationwide, and all but a few outliers have been squarely dismissed in recognition of the fact that being attacked by cybercriminals is not a fraud on investors.[3] Courts also have rejected securities fraud claims based on a company's difficulties executing a large-scale business combination and integrating the newly acquired company.[4] This case is no different, and Plaintiff has not pleaded a claim under any theory.

### A. The Complaint Fails to Plead an Actionable Misstatement or Omission

To survive a motion to dismiss, a complaint must "specify each statement alleged to have been misleading [and] the reason or reasons why the statement is misleading." *Metzler*, 540 F.3d at 1061. Statements are misleading only if they "affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists." *Brody v. Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002). "To be misleading, a statement must be 'capable of objective

---

[3] *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 31 F.4th 898 (4th Cir. 2022) (dismissing Section 10(b) claim); *Reidinger v. Zendesk, Inc.*, 2021 WL 796261 (N.D. Cal. Mar. 2, 2021) (same), *aff'd sub nom*, *Local 353, I.B.E.W. Pension Fund v. Zendesk, Inc.*, 2022 WL 614235 (9th Cir. 2022); *In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980 (N.D. Cal. 2020) (same); *Sgarlata v. PayPal Holdings, Inc.*, 409 F. Supp. 3d 846 (N.D. Cal. 2019) (same), *aff'd sub nom*, *Eckert v. PayPal Holdings, Inc.*, 831 F. App'x 366 (9th Cir. 2020); *In re Intel Corp. Sec. Litig.*, 2019 WL 1427660 (N.D. Cal. Mar. 29, 2019) (same); *In re First Am. Fin. Corp.*, 2021 WL 4807648 (C.D. Cal. Sept. 22, 2021) (same); *In re Fed Ex Corp. Sec. Litig.*, 517 F. Supp. 3d 216 (S.D.N.Y. 2021) (same); *In re Qudian Inc. Sec. Litig.*, 2019 WL 4735376 (S.D.N.Y. Sept. 27, 2019) (dismissing Section 11, 12, 15 claims).

[4] *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 543 F. Supp. 3d 96 (D. Md. 2021) (same); *Jui-Yang Hong v. Extreme Networks, Inc.*, 2017 WL 1508991 (N.D. Cal. Apr. 27, 2017) (same); *Fadia v. FireEye, Inc.*, 2016 WL 6679806 (N.D. Cal. Nov. 14, 2016) (dismissing Section 10(b) claim); *Cement Masons & Plasterers Joint Pension Tr. v. Equinix, Inc.*, 2012 WL 6044787 (N.D. Cal. Dec. 5, 2012) (same); *In re Dothill Sys. Corp. Sec. Litig.*, 2009 WL 734296 (S.D. Cal. Mar. 18, 2009) (same); *Grossman v. Novell, Inc.*, 909 F. Supp. 845 (D. Utah 1995), *aff'd*, 120 F.3d 1112 (10th Cir. 1997) (same).

verification.'" *Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.*, 845 F.3d 1268, 1275 (9th Cir. 2017) (citation omitted). Plaintiff fails to plead specific facts, as required under the PSLRA and Rule 9(b), demonstrating that any of the challenged statements about the security incident or the Auth0 integration were false or misleading.

***1. Statements Regarding Data Security and the Security Incident Are Not False or Misleading.***

Plaintiff fails to plead that any of the challenged statements relating to the importance of security to Okta or Okta's security protocols (¶¶ 19, 97, 123, 124, 143, 145, 159, 167, 168) were false or misleading.

a. Statements Regarding Okta's Commitment to Data Security.

The Court should reject out of hand Plaintiff's claim that statements about Okta's commitment to data security—e.g., that "[s]ecurity is a mission-critical issue for Okta and for our customers" (¶ 159)—were false or misleading. As the Ninth Circuit has explained, general statements about corporate commitments or values are "vague, optimistic statements [that] . . . are not actionable." *Lloyd v. CVB Fin. Corp.*, 811 F.3d 1200, 1207 (9th Cir. 2016). Courts routinely dismiss "commitment" statements as "vague, generalized assertion[s] of corporate optimism, that courts have found to be inactionable" puffery. *Extreme Networks*, 2017 WL 1508991 at *14 (citation and internal quotations omitted) (collecting cases); *see also In re Alphabet, Inc. Sec. Litig.*, 1 F.4th 687, 700 (9th Cir. 2021) ("'[T]ransparently aspirational' statements . . . are generally not actionable as a matter of law . . . ."); *First Am.*, 2021 WL 4807648, at *9 (statement that defendant "was 'committed to safeguarding customer information'" is inactionable puffery because "'commitment' is 'not a word of certainty, even when viewed in context'"). No reasonable investor would interpret Okta's statements about the importance or "mission critical" nature of security as an affirmative, verifiable statement as to any fact. Nor does the Complaint allege facts contradicting the truth of these statements about data security being important to Okta.[5]

[5] For the same reason, McKinnon's statement that he was "commit[ted] to making [Okta] a $4 billion a year company" by fiscal year 2026 is not actionable. (¶ 168.) This also is a classic protected forward-looking statement within the PSLRA safe harbor. *See In re Pac. Gateway Exch., Inc. Sec. Litig.*, 2002 WL 851066, at *9 (N.D. Cal. Apr. 30, 2002) ("Forward-looking statements are not actionable if they

*(Cont'd on next page)*

b. Statements Regarding Security Protocols.

Plaintiff challenges one statement made in an October 13, 2021 press release, which Plaintiff alleges is a quote from "the Company's Vice President of Cloud Infrastructure, Atul Bahl" regarding how "security is of the utmost importance to us," how "Okta's Custom Administrator Roles allow us to follow the principle of least privilege," and how it "ensure[s] the best-in-class security of our customer applications." (¶ 97; *see also* ¶ 145.) Plaintiff claims this statement was false and misleading because it failed to state that "Okta was not properly securing its administrative tools for monitoring customer tenants and that Okta failed to require its sub-processors to comply with the Company's fundamental security requirements." (¶ 146.)

This claim is frivolous. Plaintiff falsely claims that the statement was made by an Okta employee. It was not. As the press release Plaintiff relies on makes clear, the statement is from an Okta *customer* (Verisk), who is providing a testimonial about the importance of security to *Verisk's* business, and the value that *Verisk* realizes from Okta's products:

> "Verisk is a leading data analytics provider serving customers in insurance, energy and specialized markets, and financial services," ***said Atul Bahl, Vice President of Cloud Infrastructure, Verisk Analytics***. "As a data-focused organization, security is of the utmost importance to us. Okta's Custom Administrator Roles allow us to follow the principle of least privilege and only grant admins access to the tasks they need to perform across our many business units. We save time for our internal teams and ensure the best-in-class security of our customer applications."

(Ex. 3 at 3 (emphasis added); *see also* ¶ 145.) Obviously Okta could not have committed securities fraud through a statement made by another company.

Separately, Plaintiff claims that a statement by McKinnon—"***But then they're left—the administrative accounts or the admin or the super user accounts are left open because it's easy for the engineers to drop in there and, like, do some admin things and maintain some network things***"—was false or misleading because McKinnon allegedly omitted that "Okta was not properly securing its administrative tools" and that Okta "failed to require its sub-processors to comply with the Company's fundamental security requirements." (¶¶ 143, 144.) But Plaintiff provides no credible explanation for

---

. . . are immaterial," such as "vague statements of optimism, or 'puffery'" (citing 15 U.S.C. § 78u-5(c)(1))); *In re Copper Mountain Sec. Litig.*, 311 F. Supp. 2d 857, 880 (N.D. Cal. 2004) ("The definition of forward-looking statements includes statements containing projections of revenues . . . and predictions of future economic performance."). Moreover, this is a statement of aspiration and there are no allegations suggesting that McKinnon did not actually hold this goal.

how this statement was false or misleading. The Complaint's conclusory assertion that Okta was "not properly securing its administrative tools" is unsupported by any allegations of fact. McKinnon's statement also on its face does not even address Okta's sub-processors, so Plaintiff's contention for why it was misleading makes no sense. *See Brody*, 280 F.3d at 1006–07 (omitting information about a merger in a press release did not make it misleading because the press release "neither stated nor implied anything regarding a merger"); *see also Weller v. Scout Analytics, Inc.*, 230 F. Supp. 3d 1085, 1094 (N.D. Cal. 2017) (omitting gross revenue information from a press release did not make it misleading because "the Press Release does not mention 'gross revenue'").

Plaintiff's allegations drawn from confidential witnesses offer no help. According to Plaintiff, CW6 and CW7 believed the Company should have placed more restrictions on employee and sub-processor access to customer data. (¶¶ 146–49.) But Plaintiff pleads no facts demonstrating that these confidential witnesses—"Senior Solutions Engineers" who worked as "part of the technical sales team" (¶¶ 43, 44)—were qualified to assess whether Okta "properly secure[d] its administrative tools" (¶ 146). More importantly, neither witness identifies specific facts suggesting that any of the challenged statements were untrue. As the blog post and webpage Plaintiff cites in the Complaint make clear, the security incident had nothing to do with Okta employees or sub-processors having overbroad access to customer data.[6]

c. Risk-Factor Disclosures Regarding Data Security.

Plaintiff also fails to plead that it was false or misleading for Okta to disclose risks concerning data security in its in its annual report on Form 10-K, filed on March 7, 2022. Plaintiff points to a single bullet point in the "risk factor summary contain[ing] a high-level summary of the risk associated with [Okta's] business":

> ***An application, data security or network incident may allow unauthorized access to our systems or data or our customers' data, disable access to our service, harm our reputation, create additional liability and adversely impact our financial results.***

[6] The Complaint recounts an irrelevant incident involving one employee in the Philippines whose information allegedly was accessed by a third party as a result of "human error" (*see* ¶¶ 116–18), but that incident too is not alleged to have resulted from Okta's alleged failure to "properly secur[e] its administrative tools for monitoring customer tenants" (¶¶ 98, 144, 146).

(¶ 159.)[7] According to Plaintiff, this sentence was false or misleading because "these risks had already materialized . . . [s]pecifically, Okta had experienced the January 2022 Breach." (¶ 160.) Plaintiff also claims this sentence is actionable because "Okta omitted materially relevant facts including the January 2022 Breach." (¶ 161.)[8]

But the Complaint pleads no facts demonstrating that any data security risk *had* materialized by March 7, 2022, the date of the disclosure. The Complaint fails to allege that the actual risks identified in the disclosure—unauthorized access to Okta's or customer's data, disabled access to Okta's service, harm to Okta's reputation, liability, or adverse financial impacts (¶ 159)—"w[ere] already affecting [Okta]" at the time the disclosure was made. *Lloyd v. CVB Fin. Corp.*, 2012 WL 12883522, at *19 (C.D. Cal. Jan. 12, 2012). There are no factual allegations that, as of March 7, the security incident had disabled access to Okta's service, caused harm to Okta's reputation, resulted in any liability, or adversely impacted Okta's financial results. And as discussed further below, there are no allegations that as of March 7, Okta knew there had been any unauthorized access to Okta's or customer's data from the security incident. Thus, the "risk[s] actually warned of" had not come to fruition at the time the statement was made. *Williams v. Globus Med., Inc.*, 869 F.3d 235, 242 (3d Cir. 2017); *cf. Berson v. Applied Signal Tech., Inc.*, 527 F.3d 982, 987 (9th Cir. 2008) (risk factor disclosure was potentially misleading because the specific risk identified—cancellation of orders—had already materialized).

Nor does Plaintiff plead particularized facts showing that the risk-factor summary was false or misleading on the basis that Defendants failed to disclose "materially relevant facts" about the "January

---

[7] Plaintiff does not challenge as false or misleading the detailed, five-paragraph risk factor that appears later in the Form 10-K, which further describes the summary risk factor Plaintiff challenges. (*See* Ex. 4 at 27–28.)

[8] Plaintiff also challenges two statements from the same Form 10-K that Plaintiff falsely describes as risk factors: (i) "Security is a mission critical issue for Okta and for our customers"; and (ii) "We ensure that access to our platform is securely delegated across an organization." (¶ 159.) The first statement also is inactionable puffery because it is a "vague, optimistic statement" about the values that are important to Okta. *See Lloyd*, 811 F.3d at 1207 (statement that "strong credit culture and underwriting integrity remain paramount" is puffery). And without details on what it means for a platform to be "securely delegated across an organization," the second statement is "'simply too vague to constitute a material statement of fact.'" *First Am.*, 2021 WL 4807648, at *10 (quoting *Searles v. Glasser*, 64 F.3d 1061, 1066 (7th Cir. 1995)).

2022 Breach." (¶ 161.) According to Plaintiff, "Defendants admitted that they were aware of this breach in January 2022" (*id.*), and they "sat on this information for almost two months" (¶ 111). But this omissions theory is premised on a fundamental mischaracterization of both the security incident itself and Plaintiffs' own pleading. The Complaint cites and relies on a March 25, 2022 FAQ document that refutes Plaintiff's baseless claim that Defendants knew of, and failed to disclose, a known data breach:

> In January, we did not know the extent of the Sitel issue – only that we detected and prevented an account takeover attempt and that Sitel had retained a third party forensic firm to investigate. At that time, we didn't recognize that there was a risk to Okta and our customers.

(Ex. 6 at 4.) *None* of the confidential witnesses cited in the Complaint say that any of the Individual Defendants even were aware of the security incident in January 2022. Plaintiff has pleaded no facts to support its claim that the risk-factor disclosure was misleading on account of Defendants' failure to disclose a known security incident in January 2022.

In fact, during the entire period relevant to this case—and still at the time of this submission—the SEC did not, and does not, impose any general duty to disclose cybersecurity incidents. Although the SEC has proposed promulgating new rules on such disclosures, even under that proposal companies would have no duty to disclose an incident before it is determined to be material. *Cf.* SEC, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule, 87 Fed. Reg. 16,590, 16,595–96 (proposed Mar. 23, 2022) (to be codified at 17 C.F.R. §§ 229 *et seq.*) ("We are proposing that the trigger [for a duty to disclose] is the date on which a registrant determines that a cybersecurity incident it has experienced is material, *rather than the date of discovery of the incident*, so as to focus the . . . disclosure on incidents that are material to investors. In some cases, . . . the materiality determination will come after the discovery date." (emphasis added)). Thus, even under the proposed rule the SEC has not yet promulgated, Plaintiff has failed to plead facts showing that Okta would have been required to disclose the data security incident because there are no specific factual allegations that Okta was aware of a breach—let alone a material one—by March 2022.

Finally, even viewing the incident (impermissibly) with hindsight only underscores its immateriality. According to the documents Plaintiff cites to and relies on in the Complaint, the hacker

never breached Okta's systems, never obtained sensitive Okta customer data, and Plaintiff has pleaded no facts contradicting the Company's statement in the earnings call Plaintiff cites in the Complaint that the incident had no "quantifiable impact" on Okta's financial performance. (Ex. 8 at 4 ("I'm sure this audience is wondering what impact the security incident had on our financial results. While we've done a lot of analysis, it's difficult to attribute any quantifiable impact on our solid Q1 results."); Lutz Dec. at ¶ 10 ("A lot of people said you would lose customers. This was the strongest customer retention that I've seen you have and it made [you] new customers. So it's obvious that whatever anybody thought, your loss of trust didn't exist . . . . and yet [you] w[o]n over even more clients.").)

This case is nothing like *Alphabet*, where the Ninth Circuit concluded that a risk factor about cybersecurity risks was adequately alleged to be misleading. Alphabet was alleged to have been aware of an undisclosed security vulnerability that existed for years and affected hundreds of thousands of Google's users. *Alphabet*, 1 F.4th at 693, 702–04. The Complaint alleged specific facts demonstrating that the security vulnerability had been investigated and reported in a detailed memo provided to Google's senior-most officers, who were alleged to have known about the security vulnerability but caused Alphabet and Google to state publicly that no such vulnerability existed. *Id.* at 695–96. In stark contrast to those allegations, the security incident here involved the system of a third party (not Okta), impacted only a tiny fraction of Okta's customers, and is not alleged to have been known by Okta's senior officers at the time Okta disclosed the challenged risk factor. (*See supra*, p. 6–7.)

For all these reasons, Plaintiff has failed to plead particularized facts demonstrating that the summary risk-factor statement (or any statement falsely described as a risk-factor statement) was false or misleading.

d. McKinnon's Statements Regarding January 2022 Security Incident.

Plaintiff also fails to plead facts demonstrating that McKinnon's statement on June 8, 2022 regarding feedback he had received from customers about the security incident was false or misleading. (*See* ¶¶ 19, 123, 167 ("We talked to over 1000 customers . . . . I . . . got a ton of feedback about what we could do better, how we could make sure that our support environment was not insecure, to make sure that we communicate better, to make sure that we are instill this trust. At the end of the [day], I think we've been able to do that.").) Plaintiff alleges these statements were misleading because they

failed to disclose that "Okta was actually losing sales as a direct result" of the security incident. (¶¶ 125, 169.) This claim fails for multiple reasons.

Plaintiff fails to plead facts drawing any connection between the alleged misstatement—McKinnon's report of feedback he received from customers—and the purported reason Plaintiff claims the statement was misleading—namely, that Okta was "losing sales" as a result of the security incident. (¶ 169.) Even if Plaintiff's unsupported and conclusory allegation were accurate, the loss of sales by Okta would not contradict statements about general feedback McKinnon received from customers. *See Metzler*, 540 F.3d at 1061 ("By requiring specificity," the PSLRA requires a plaintiff to provide a "particularized explanation stating *why* the defendant's alleged statements . . . are deceitful").

Additionally, McKinnon's belief that "I think we've been able to do that"—meaning "do better," create a secure "support environment," "communicate better," and "instill this trust"—is also inactionable puffery and opinion, and Plaintiff alleges no facts showing McKinnon did not believe what he said. *See Rodriguez v. Gigamon Inc.*, 325 F. Supp. 3d 1041, 1054 (N.D. Cal. 2018) ("Puffery is an expression of opinion," and "[g]eneralized statements of corporate optimism . . . may be considered puffery" (citing cases)); *In re QuantumScape Sec. Class Action Litig.*, 580 F. Supp. 3d 714, 738–39 (N.D. Cal. 2022) (statements of opinion, such as those prefaced with "I think," do not "express[] certainty about a thing" and are not material misrepresentations unless the plaintiff "allege[s] . . . that the speaker did not hold the belief she professed and that the belief is objectively untrue"). Plaintiff also fails to plead facts supporting the conclusory allegation that Okta had lost sales because of the security incident, such as by identifying a customer that did not renew or sign a contract because of the incident. Anecdotal opinions from confidential witnesses about customer reactions to the incident and Plaintiff's unsupported conclusion that Okta "was losing sales as a direct result" of the incident (¶¶ 125, 69) do not make it so, and do not render McKinnon's general opinion about customer feedback false or misleading.

Finally, Plaintiff's challenge to McKinnon's statement about Okta's goal to "capture this market opportunity" and meet its financial projections (¶¶ 124, 168) also fails. This statement concerns the balance between growth and cash flow—it has nothing to do with data security or the security incident, and therefore cannot be misleading by not addressing those issues. *See Brody*, 280 F.3d at

1006–07 (omission of information from a statement does not render the statement misleading if the statement does not speak to that issue). This statement also is inactionable puffery and opinion about the Company's plans, and Plaintiff pleads no facts suggesting that McKinnon did not actually hold his belief that Okta planned to achieve these goals. *See QuantumScape*, 580 F. Supp. 3d at 738–39.

***2. Statements Regarding the Auth0 Integration Are Not False or Misleading.***

Plaintiff also fails to plead that Defendants made a false or misleading statement about integrating Auth0.

a. Statements of Optimism Regarding the Progress of the Auth0 Integration.

Most of Plaintiff's challenges relate to generic statements of optimism regarding the progress of the Auth0 integration. These are not actionable for several reasons.

*First*, the challenged statements are classic puffery, not verifiable facts that can be proven true or false. (*See, e.g.*, ¶ 134 ("we're off to a fantastic start"), ¶ 135 ("when you think about us plus Auth0, it is going very well"), ¶ 140 ("the integration has gone very well"), ¶ 142 ("We're benefiting a lot on that from . . . the acquisition of Auth0"), ¶ 150 ("We're maintaining the momentum of both Okta and Auth0 and are making great progress on the integration"), ¶ 151 ("it's going very well"), ¶ 155 ("We are off to a great start"), ¶ 157 ("What we're getting is we're getting synergy . . . on the sales side. . . . [T]here's a ton of upside from that."), ¶ 162 ("We've made a lot of progress as a combined company. . . . I think we've made great progress"), ¶ 163 ("It was a great milestone for us . . . and we're pleased with the progress, thus far.").) These generic statements are "textbook examples of non-actionable puffery and corporate optimism that are not capable of objective verification or inducing reliance of a reasonable investor." *Welgus v. TriNet Grp., Inc.*, 2017 WL 6466264, at *11 (N.D. Cal. Dec. 18, 2017), *aff'd*, 765 F. App'x 239 (9th Cir. 2019); *see also In re Cutera Sec. Litig.*, 610 F.3d 1103, 1111 (9th Cir. 2010) ("optimistic, subjective assessment[s] hardly amount[] to a securities violation," and instead constitute "non-actionable puffing"). "CEOs and executives of companies that . . . acquire other

companies often describe ongoing mergers as smooth, rapid, and successful—which courts regularly deem corporate puffery." *FireEye*, 2016 WL 6679806, at *7.[9]

*Second*, Defendants' statements about their progress integrating Auth0 were not false or misleading in light of "the context in which [the statements] were made, specifically in regard to contemporaneous qualifying or clarifying language." *Intel*, 2019 WL 1427660, at *10. Defendants repeatedly emphasized that integrating the sales teams was difficult, that there was work to be done, and that the process would take time:

- On a September 2021 earnings call, Defendants acknowledged that they "didn't have all the answers," and that there were many "important point[s]" relating to employee retention that they were "thinking about as we go forward." (¶¶ 74, 136.)
- During the December 2021 earnings call, Defendants emphasized that they could not "just flip the switch" to successfully integrate the companies, that there was "a lot on [Okta's] plate," and that there was "a lot of work" to be done on "getting all the new folks ramped on now the broader suite of products that they're going to have to offer." (¶¶ 85, 151.)
- In a March 2022 earnings call, Defendants again stated "there is still a lot of work to do," and that there were "a couple more pieces we need to finish up." (¶¶ 93, 155, 156.)
- And even in June 2022, Defendants explained that "there's no real finish line when it comes to integrations," and that although the acquisition had closed a year earlier, "[t]here's still a little bit to do." (¶¶ 120, 162.)

"Analysis of the statements made about the merger process must fairly consider the context in which the statements were made, and representations made regarding the entirety of the complex overall process are a far cry from specific representations about one detailed aspect of the much larger whole." *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 543 F. Supp. 3d 96, 114 (D. Md. 2021). Here, given the entirety of Defendants' statements concerning integrating the $6.5 billion Auth0 business into Okta, no reasonable investor could have been misled into believing the integration process was unassailably successful. Plaintiff's claim that there were setbacks in the sales integration (such as

[9] Many of the challenged statements also are inactionable statements of opinion. (*See, e.g.*, ¶ 140 ("So the integration has gone very well. We're about 4 months in. We're pretty good at execution. So we had some pretty good goals for ourselves, but *I think* we've been beating even those, which is great."), ¶ 162 ("So *I think* we've made great progress. There's still a little bit to do, but we're in good shape."); ¶ 163 ("It was a great milestone for us . . . and *we're pleased* with the progress, thus far.") (emphases added).) These opinion statements "inherently reflect the speaker's assessment of and judgment about the underlying circumstances," *Markette v. XOMA Corp.*, 2017 WL 4310759, at *4 (N.D. Cal. Sept. 28, 2017), and are not material misrepresentations absent an allegation that the speaker did not actually hold these beliefs, *QuantumScape*, 580 F. Supp. 3d at 738–39. Plaintiff has not pleaded no such facts.

employee retention and salesforce unification) does not turn Defendants' statements about integration into fraud.

*Third*, the premise of Plaintiff's falsity theory—that employee attrition and retention challenges undermined the sales team's ability to sell products—is unsupported by particularized facts. The Complaint's *only* allegation about specific employee departures comes from CW1, who stated that in August 2021—*before the start of the alleged class period*—Auth0's former Chief Legal Officer, Chief Human Resources Officer, Chief Financial Officer, and Chief Revenue Officer left the combined company. (¶ 65.) These departures are not alleged to have had any bearing on the problems Okta is alleged to have experienced integrating the sales function the following year. Nor has Plaintiff alleged that these senior-level departures were unexpected from an integration planning perspective.

Plaintiff's reliance on allegations from other confidential witnesses about employee retention issues is even weaker. According to CW4, "attrition was a 'common concern'" and "employees started to leave Okta" (¶ 66), but this witness does not identify who shared this "common concern"; does not describe how many employees left, their titles, or their dates of departure; and does not say whether any Individual Defendant was aware of the concern and when. Plaintiff provides no specific facts connecting CW4's vague concerns about attrition to Okta's ability to successfully integrate the sales teams. *See FireEye*, 2016 WL 6679806, at *10 (plaintiff's "fail[ure] to provide details regarding the extent and severity of layoffs" meant there would not have been "a significant alteration in the total mix of information available to reasonable investors"). Similarly, CW5's allegation that "all of the 'founding fathers' of Okta as well as . . . approximately 75–80% of the VPs and SVPs" left the Company (¶ 67) also lacks specific facts demonstrating that the challenged statements about Auth0 integration were false or misleading. Again, there are no facts pleaded about whether these "VPs and SVPs" were involved in sales, when they left, or how their departures rendered Okta's statements about integrating the sales team false.

Also missing from the Complaint are particularized facts about the specific timing of alleged employee departures vis-à-vis the challenged statements in September 2021, December 2021, March 2022, and June 2022—a telling defect that prevents the Court from "determin[ing] the temporal relationship between [the witness]'s statements and [the challenged] statements." *Brodsky v. Yahoo!*

*Inc.*, 630 F. Supp. 2d 1104, 1114 (N.D. Cal. 2009); *see also Extreme Networks*, 2017 WL 1508991, at *16 (the fact that a witness "personally observed or experienced the Company's integration efforts" is "insufficient" when they only "reflect generally on difficulties experienced with the overall integration" and "do not speak directly to the falsity of the alleged statements when made"). Without detailed supporting facts, Plaintiff's allegations about employee retention and attrition issues "are not inconsistent with the [Defendants'] statements so as to show that the statements must have been false or misleading when made." *Ronconi v. Larkin*, 253 F.3d 423, 434 (9th Cir. 2001).

At bottom, all that Plaintiff has vaguely alleged is that there were general challenges relating to employee retention and unification of the sales teams. At no time, however, did Defendants ever state that the Auth0 sales integration was progressing perfectly and without any challenges. To the contrary, Defendants acknowledged throughout the relevant period that the integration was a work in progress. And as the Ninth Circuit has noted, general allegations that the integration of sales teams after a merger was "not as productive a maneuver as [defendants] had hoped" "do not meet the level of specificity required by the PSLRA and our caselaw interpreting it." *Id.* at 434. "Problems and difficulties are the daily work of business people," and "[t]hat they exist does not make a lie out of any of the alleged false statements." *Id.*; *see also Brodsky*, 630 F. Supp. 2d at 1113 (merely "[a]lleging a litany of problems" regarding the integration of an acquired company is not enough to prove the falsity of statements that "project optimism").

b. Risk-Factor Disclosures Regarding the Auth0 Acquisition.

Plaintiff's attempt to cast Okta's risk-factor disclosures regarding the Auth0 acquisition as misstatements fails. (*See* ¶¶ 138, 153, 159, 165.) As explained above, Okta warned investors that the integration would take time and that the success of the acquisition was not guaranteed (*see supra*, p. 17.) Okta also identified the risks that "a loss of our and/or Auth0's key employees and customers" and that "[t]he ongoing integration process may require significant time and resources, and [the Company] may not be able to manage the process successfully." (¶¶ 138, 153, 159, 165.)

These risk factors disclosed the very challenges Plaintiff now claims were concealed. Plaintiff nonetheless argues these statements were misleading "because these risks had already materialized" at the time of the risk factor statements. (¶¶ 139, 154, 160, 166.) Plaintiff is wrong.

The risk-factor disclosures were not false or misleading because Plaintiff does not plead any specific facts showing these risks had "come to fruition" when the disclosures were made in September 2021, December 2021, March 2022, or June 2022 (*see* ¶¶ 138–39, 153–54, 159–60, 165–66). *Siracusano v. Matrixx Initiatives, Inc.*, 585 F.3d 1167, 1181 (9th Cir. 2009), *aff'd*, 563 U.S. 27 (2011). To the contrary, Defendants explained to investors on numerous occasions throughout the relevant period that it would take time for the integration process to play out. Although the acquisition closed in May 2021, the unification of the sales teams did not occur until nine months later, in February 2022. (*See* ¶¶ 73, 78, 93, 94.) Even then, Defendants acknowledged in March 2022 that they were "continu[ing] to refine our systems and processes," and conceded there was "still a lot of work to do." (¶ 93.) As CW3 acknowledged, even as late as in the first two quarters of 2023 (i.e., February to July 2022), it remained unclear whether the integration of the sales team would have an adverse impact on sales performance: at first, although CW3 "only managed to achieve 20% of her quota," other "team members did better." (¶ 40.) The Company then implemented "performance plan[s]" to improve sales, and by the next quarter (i.e., May to July 2022), "she started to get more sales opportunities." (*Id.*) CW3's own experience contradicts Plaintiff's unsupported theory that the risks associated with integrating Auth0 had, at some unspecified time, already "come to fruition." Without any specific allegations to the contrary, there is no basis to conclude that these risks had materialized in any meaningful way when the risk disclosures were made.

### B. The Complaint Fails to Adequately Plead a Strong and Compelling Inference of Scienter

The PSLRA requires a securities plaintiff to plead "with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind" for "each [misstatement] or omission." 15 U.S.C. § 78u-4(b)(2)(A). An inference of scienter is "strong" if it is "cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007). In the Ninth Circuit, the plaintiff bears the burden of pleading facts that support a strong inference that "'the defendants made false or misleading statements either intentionally or with deliberate recklessness.'" *Sgarlata*, 409 F. Supp. 3d at 853 (quoting *Zucco*, 552 F.3d at 991). "Recklessness only satisfies scienter under § 10(b) to the extent that it reflects some

degree of intentional or conscious misconduct." *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1053 (9th Cir. 2014) (internal quotation marks omitted). Where the plaintiff relies on an omissions theory, the plaintiff must further plead particularized facts demonstrating "an extreme departure from the standards of ordinary care, and which presents a danger of misleading buyers or sellers that is either known to the defendant or is so obvious that the actor must have been aware of it." *Zucco*, 552 F.3d at 991 (internal quotation marks omitted). Scienter must be pleaded with particularity as to *each* defendant. *In re VeriSign, Inc., Deriv. Litig.*, 531 F. Supp. 2d 1173, 1207 (N.D. Cal. 2007) ("It is not sufficient under the PSLRA to allege scienter against defendants as a group."). This is an "exacting pleading obligation" with "teeth." *Nguyen v. Endologix, Inc.*, 962 F.3d 405, 414 (9th Cir. 2020) (quoting *Zucco*, 552 F.3d at 990).

The Complaint falls far short of pleading the specific facts necessary to support a strong inference that any Defendant knew or was deliberately reckless in not knowing that their statements about the security incident and the Auth0 integration were false or misleading. Plaintiff's scienter argument boils down to the bare assertion that the Individual Defendants must have known the challenged statements were false or misleading simply because security and the Auth0 acquisition were important to Okta. (*E.g.*, ¶¶ 207–23.) These allegations come nowhere near the specificity required to plead scienter under the PSLRA's heightened standard.

***1. The Confidential Witness Statements Do Not Give Rise to a Strong Inference of Scienter.***

The Complaint cites allegations purportedly drawn from confidential witnesses in a failed attempt to plead scienter. The Ninth Circuit applies a two-part test for determining whether confidential witness allegations support a strong inference of scienter: (1) "whether a complaint has provided sufficient detail about a confidential witness' position within the defendant company to provide a basis for attributing the facts reported by that witness to the witness' personal knowledge" and (2) whether "those statements which are reported by confidential witnesses with sufficient reliability and personal knowledge [are] themselves . . . indicative of scienter." *Zucco*, 552 F.3d at 995. Plaintiff's allegations fail at each step.

a. The Confidential Witness Allegations Fail to Support an Inference of Scienter with Respect to the Security Incident Statements.

The allegations supposedly drawn from three confidential witnesses—CW6, CW7, and CW9—relating to data security fail to support an inference of scienter because these witnesses had no connection with the Individual Defendants, and the information they purportedly provided has nothing to do with the relevant question: "whether the [Individual Defendants] knew [their] statements were false, or w[ere] consciously reckless as to their truth or falsity." *Gebhart v. SEC*, 595 F.3d 1034, 1042 (9th Cir. 2010).

These confidential witnesses are not alleged to have had any personal knowledge of the Individual Defendants' state of mind at any time, including when the alleged misstatements were made. *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, 759 F.3d 1051, 1063 (9th Cir. 2014) ("witness statements . . . lack foundation" because "the witnesses lack first hand knowledge regarding what the individual defendants knew or did not know about" allegedly omitted information). In fact, CW6, CW7, and CW9 each left Okta *before* any of the challenged statements concerning the security incident were made. (*Id.* ¶¶ 43–44, 46.) These witnesses, therefore, are not alleged to have any personal knowledge of the security incident, the security measures Okta employed in January 2022, or how Okta secured its "SuperUser" accounts after they were no longer employed by the Company—let alone personal knowledge of what the Individual Defendants knew about these issues. *See In re Intrexon Corp. Sec. Litig.*, 2017 WL 732952, at *6 (N.D. Cal. Feb. 24, 2017) (confidential witness allegations "fail to establish personal knowledge and reliability" where "the witnesses were not employed during the class period"). And even when they allegedly were still employed by Okta, not one of these confidential witnesses is alleged to have reported to, worked with, or even spoken with any Individual Defendant. (¶¶ 98–102, 113–18.) Thus, these witnesses are unreliable and the allegations attributed to them fail to support an inference of scienter.

In any event, the allegations drawn from these confidential witnesses are irrelevant to scienter with respect to any Defendant. None of the allegations attributed to CW6, CW7, and CW9 relate to the security incident, and their opinions about Okta's general data security practices do not inform whether Defendants made any supposed misstatements deliberately or recklessly. For example, CW9 is alleged to believe the security incident was "not surprising" because of a separate incident in October

2021, when a third party gained access to CW9's data due to "human error." (¶ 118.) But Plaintiff pleads no facts that the two incidents were connected in any way, or that knowledge of the earlier incident would have put anyone on notice that the later security incident might occur. Nor can CW6's and CW7's *opinions* about security measures Okta should have implemented support any inference of scienter with respect to any Defendant. *See In re Intrexon*, 2017 WL 732952, at *6 (confidential witness's opinions about a company's product "fail to suggest scienter"); *Metzler*, 540 F.3d at 1069 (internal "disagreement and questioning" about accounting method insufficient to establish scienter).

b. The Confidential Witness Allegations Fail to Support an Inference of Scienter with Respect to the Auth0 Integration Statements.

The confidential witness allegations relating to the Auth0 integration also do not support any inference of scienter. Plaintiff again pleads no facts demonstrating that any witness had first-hand knowledge of any Individual Defendant's state of mind with respect to the Auth0 sales integration. No witness is alleged to have reported to, spoken with, or provided information to any Individual Defendant about the integration of the Okta and Auth0 sales teams. (*See* ¶¶ 38–46, 63–68, 78–83, 88–92.) Instead, the confidential witnesses offer only unreliable hearsay (*e.g.*, *id.* ¶ 221), conclusory assertions about what the Individual Defendants supposedly must have known (*e.g.*, *id.* ¶¶ 217–19, 221, 223), or vague allegations about McKinnon's attendance at weekly "All Hands" meetings (*e.g.*, *id.* ¶¶ 218–19). Even CW2, who had supposedly been "'intimately involved' with the Auth0 and Okta integration" and "put[] together the integration plan," is not alleged to have ever had a direct conversation with any Individual Defendants about employee attrition and its impact on the sales function, or challenges with cross-selling in the unified sales force. (¶ 217.) For this reason alone, the confidential witness allegations fail to support any inference of scienter with respect to the Auth0 integration statements. *See Johnson v. Costco Wholesale Corp.*, 2020 WL 4816225, at *6 (W.D. Wash. Aug. 19, 2020) (concluding allegations drawn from a confidential witness did not support scienter because he did not allege "any direct contact with or reliable personal knowledge regarding what [the defendants] knew at the time").

Nor are any of the confidential witness allegations themselves indicative of scienter with respect to the Auth0 integration. For example, Plaintiff alleges that Okta held "weekly calls [that] occurred

throughout the planning period," but Plaintiff pleads no facts from a confidential witness or otherwise that any of the Individual Defendants participated in these calls, what was discussed during these calls, or when these calls purportedly occurred. (¶¶ 80, 217.) *See also Kang v. PayPal Holdings, Inc.*, --- F. Supp. 3d ---, 2022 WL 3155241, at *11 (N.D. Cal. Aug. 8, 2022) (rejecting confidential witness allegation about "undated 'weekly or biweekly meetings' where 'updates were provided'" without "attest[ing] to any Individual Defendant ever attending a meeting or receiving a report about" the allegedly concealed information). Nor does CW2's allegation that the "integration model was 'ripped out' at the 'eleventh hour'" by the "finance team" support any inference of scienter for any Defendant. (¶ 81.) A "change in business strategy does not, without more, render . . . past disclosures" about the progress of the integration misleading. *In re Diebold Nixdorf, Inc., Sec. Litig.*, 2021 WL 1226627, at *11 (S.D.N.Y. Mar. 30, 2021). "A company may shift gears for any number of reasons, most of which have nothing to do with fraud." *Id.*

Plaintiff's allegation, drawn from CW3 and CW5, that McKinnon held weekly "all-hands meetings" (¶¶ 218–19), fares no better. CW3 offers no details about these meetings. CW5 claims that "integration issues were discussed," including "problems making sales for Auth0" (¶ 219), but CW5 does not allege *when* during CW5's three-year tenure at the Company these meetings occurred. More importantly, CW5 pleads no facts suggesting that at these meetings McKinnon discussed or learned information that contradicted his public statements about the Auth0 integration. Simply discussing "integration issues" or "problems making sales for Auth0" is unsurprising given Defendants' repeated acknowledgment that there was more work to do on the sales integration—and a far cry from specific facts raising a strong inference that McKinnon knew the Company's public statements about the sales integration were false. *See Colyer v. AcelRx Pharms., Inc.*, 2015 WL 7566809, at *9 (N.D. Cal. Nov. 25, 2015) ("Plaintiffs have failed to explain how [d]efendants' knowledge of [product errors] would necessarily translate into knowledge . . . [of] a significantly higher risk of rejection by the FDA.").

The remaining confidential witness allegations—which consist of their opinions about the Auth0 integration strategy and two new executives (*e.g.*, ¶¶ 63–68, 78–83); vague and generalized statements of a "mass exodus" and unidentified employees' concerns about attrition (*e.g.*, ¶¶ 63–68, 88–92); and employees' alleged difficulties selling both Auth0 and Okta products (*e.g.*, ¶¶ 88–92)—

also fail to demonstrate the "direct" or "personal" involvement of any of the Individual Defendants in the sales integration, much less allow the Court to draw a cogent and compelling inference that Defendants knew or were deliberately reckless in not knowing that their statements about the sales integration were false or misleading.

For example, Plaintiff alleges that CW1 was "'confident' [that] McKinnon and Pace were having discussions about the integration of Okta and Auth0." (¶ 221.) Based on this, and nothing more, Plaintiff leaps to the conclusion that "there is no question that [former Auth0 CEO Eugenio] Pace would be aware of the integration issues . . . , especially the increased attrition for Auth0 employees," and this knowledge must have been shared with McKinnon because of their "strong" relationship, their "respective roles at Okta," and because Pace reported to McKinnon. (¶¶ 220–21.) Plaintiff offers no particularized factual basis to substantiate CW1's unsupported belief about these two individuals whom CW1 is not alleged to have reported to, spoken with, or even met. Similarly, CW1's allegation that she heard from some unknown source that the board was reviewing attrition numbers and was "very concerned" is hearsay, and unreliable under the Ninth Circuit's test for assessing the credibility of confidential witness statements. *See Zucco*, 552 F.3d at 997.

***2. Plaintiff's "Core Operations" Allegations Do Not Support Scienter.***

Plaintiff cannot satisfy the heightened standard for pleading scienter by claiming the Defendants must have known their statements were false because "[s]ecurity is a mission critical issue for Okta" (¶ 159), and the Auth0 integration was "critical to Okta's operations and growth" (¶ 207). This attempt to plead scienter by invoking the core operations doctrine fails.

"The core operations theory of scienter relies on the principle that 'corporate officers have knowledge of the critical core operation of their companies.'" *Intuitive Surgical*, 759 F.3d at 1062 (quoting *Reese v. Malone*, 747 F.3d 557, 569 (9th Cir. 2014)). Such "core operation" allegations must typically be accompanied by "detailed and specific allegations about management's exposure to factual information within the company." *S. Ferry LP*, 542 F.3d at 785; *see also id.* at 784–85 ("Where a complaint relies on allegations that management had an important role in the company but does not contain additional detailed allegations about the defendants' actual exposure to information, it will usually fall short of the PSLRA standard."); *Metzler*, 540 F.3d at 1068 ("[C]orporate management's

general awareness of the day-to-day workings of the company's business does not establish scienter—at least absent some additional allegation of specific information conveyed to management and related to the fraud."). In "exceedingly rare" and "unusual" cases, core operations allegations alone can support an inference of scienter if "the nature of the relevant fact is of such prominence that it would be 'absurd' to suggest that management was without knowledge of the matter." *S. Ferry LP*, 542 F.3d at 785–86 & n.3. Under either test, Plaintiff comes nowhere close to pleading scienter under the core operations doctrine.

First, Plaintiff fails to plead facts demonstrating that the Individual Defendants had access to reports or other information relating to the security incident that would have informed them that their statements were false or misleading. *Intuitive Surgical*, 759 F.3d at 1063 ("Missing are allegations linking specific reports and their contents to the executives, not to mention the link between the witnesses and the executives."). The Individual Defendants are not even alleged to have known about the security incident before the hacker publicly posted the screenshots from the Okta sub-processor's computer. Nor does the statement that "[s]ecurity is a mission critical issue for Okta" (¶ 159) make this the rare case where it would be "absurd to suggest" that Okta's senior officers were aware of information—whether related to this particular security incident or otherwise—demonstrating that Okta's public statements about data security were false or misleading. *See S. Ferry LP*, 542 F.3d at 785–86 & n.3.

Plaintiff also claims that "[g]iven the importance of the Auth0 acquisition to Okta's business, knowledge of the integration problems can therefore be imputed to the Individual Defendants." (¶ 215.) But here again, the Complaint lacks "detailed and specific allegations" that the Individual Defendants had access to information demonstrating that any of the challenged statements about the Auth0 integration were false or misleading. *S. Ferry LP*, 542 F.3d at 785. Plaintiff pleads no facts demonstrating "what was said by the parties in . . . meetings," with respect to the integration, "which facts the Defendants were exposed to" regarding integration, or "why this exposure supports an inference of scienter." *FireEye*, 2016 WL 6679806, at *16. At most, Plaintiff alleges, based on information purportedly provided by CW5, that the Individual Defendants, "in particular . . . McKinnon," could access "Customer Relationship Management tools that closely monitored sales to

new customers" and that "one could figure out revenue from deals by analyzing the information" in these tools. (¶ 223.) But nowhere does Plaintiff allege that information available in this tool contradicted any challenged statement about the sales integration. *See Johnson*, 2020 WL 4816225, at *7 ("[A]bility to access information, as Plaintiffs allege here, is not enough to satisfy scienter pleading requirements.").

Second, Plaintiff fails to plead facts showing that this is one of the "exceedingly rare" cases where it would be absurd to suggest that the Individual Defendants did not know the statements about the integration were false or misleading when made. *S. Ferry LP*, 542 F.3d at 785 n.3. This is a high bar that requires plaintiffs demonstrate that the falsity of the alleged misstatements was so "patently obvious" that "the defendants' awareness of the information's falsity can be assumed." *Zucco*, 552 F.3d at 1001.

Plaintiff has not—and cannot—plead facts to satisfy this high standard. For starters, the allegedly false statements about the progress of the sales integration are inactionable statements of corporate optimism. (*E.g.*, ¶¶ 134, 135, 140, 142, 150, 151, 155, 156, 162, 163.) These are simply not the kind of objectively verifiable statements where it would be "patently obvious" if they were false. *See Berson*, 527 F.3d at 989 ("Where defendants make cheerful predictions that do not come to pass, plaintiffs may not argue, based solely on defendants' prominent positions in the company, that they ought to have known better."); *Ronconi*, 253 F.3d at 432 ("Honest optimism followed by disappointment is not the same as lying or misleading with deliberate recklessness.").

Plaintiff also does not allege with particularity that the allegedly adverse information about the sales integration was so dramatic and prominent that it had to have been known by the Individual Defendants, and necessarily rendered their general (and qualified, *see, e.g.*, ¶¶ 74, 85, 93, 136, 151, 155, 156) statements about the integration progress false or misleading. The Complaint is silent as to how many employees left Okta, whether they were all sales personnel, and how those departures compared to Okta's total number of employees or normal attrition rates, or otherwise quantify the significance of the sales issues. *See Ronconi*, 253 F.3d at 432 ("Nowhere does plaintiffs' complaint state what these 'significant' or 'difficult' problems were or how they show that the two companies were operating separately at a time when they were claimed to have been consolidated."). All Plaintiff

has alleged is that the Individual Defendants were aware of and involved in the integration of Auth0. This is plainly insufficient to plead that it would be absurd to suggest that the Individual Defendants were unaware that any of the challenged statements were false or misleading. *City of Dearborn Heights Act 345 Police & Re. Sys. v. Align Tech., Inc.*, 65 F. Supp. 3d 840, 859 (N.D. Cal. 2014) (rejecting core operations doctrine based on allegations of defendants' positions and close involvement in an acquisition and integration).

***3. The Challenged Integration Statements Do Not Support a Strong Inference of Scienter.***

Plaintiff also claims that scienter should be inferred merely because the Individual Defendants made the challenged statements about the Auth0 integration. This argument is nonsensical.

The PSLRA's heightened standard for pleading scienter would be meaningless if plaintiffs could plead fraudulent intent based simply on the fact that the defendants made the alleged misstatements. *See In re Federated Dep't Stores, Inc., Sec. Litig.*, 2004 WL 444559, at *7 (S.D.N.Y. Mar. 11, 2004) ("Plaintiffs cite no case for the doubtful proposition that scienter can be inferred merely from the allegedly fraudulent statements themselves. Such a result would eliminate the need to plead scienter."); *Reidinger*, 2021 WL 796261 at *10 ("The scienter requirement exists because falsity does not always equal fraud."); *cf. In re BellSouth Corp. Sec. Litig.*, 355 F. Supp. 2d 1350, 1374 (N.D. Ga. 2005) (describing as "circular" plaintiff's argument that "this [fraudulent] conduct occurred and that its occurrence itself evidences each defendant acted with scienter").

Regardless, Plaintiff's attempt to plead scienter based on the integration statements themselves suffers from a basic pleading failure described above: there are no factual allegations showing that any of the Individual Defendants had knowledge of contemporaneous information demonstrating that any of their statements about the Auth0 integration were untrue. *See, e.g., In re SolarCity Corp. Sec. Litig.*, 274 F. Supp. 3d 972, 1012 (N.D. Cal. 2017) (no scienter because defendants' statements about company's forecasting model and goals were not particular enough to suggest that defendants accessed data regarding all project or forecasting models); *In re Am. Apparel, Inc. S'holder Litig.*, 855 F. Supp. 2d 1043, 1081 (C.D. Cal. 2012) (no scienter because defendants' statements were "too vague" or "too attenuated" without facts alleging contemporaneous receipt of directly contradictory information).

For example, Plaintiff points to a statement shortly after the acquisition that Okta was "making great progress on the integration" (¶ 227), and later, that "[w]e are off to a great start and recognize there is still a lot of work to do" (¶ 228). But the Complaint fails to plead specific facts demonstrating that at the time of these statements, the Defendants were in possession of information demonstrating that Okta was *not* making great progress on the integration, that Okta was *not* off to a great start, or that Okta did *not* recognize there was still work to do. In fact, one confidential witness agreed that the integration *did* "beg[i]n as promising." (¶ 78.) *See supra*, Section V.A.2. Nothing about these statements—which are immaterial puffery in any event—suggests that any Defendant knew their statements about the integration were false or misleading when made.

***4. The Complaint Fails to Plead Corporate Scienter.***

Plaintiff contends that the scienter of two executives who are not defendants—namely, Susan St. Ledger (Okta's head of field operations) and Steve Rowland (Okta Chief Revenue Officer)—can be imputed to Okta. Plaintiff, again, is wrong.

First, Plaintiff fails to plead facts demonstrating that either of these two non-defendants were aware that Okta's public statements were false or misleading. St. Ledger and Rowland allegedly "were involved in the weekly status updates" and "'signed off on everything.'" (¶¶ 80, 217.) That is a far cry from detailed facts demonstrating that these two non-defendants knew Okta's statements about the sales integration were false. *See In re Mellanox Techs. Ltd. Sec. Litig.*, 2014 WL 12650991, at *19 (N.D. Cal. Mar. 31, 2014) (rejecting confidential witness allegations about "hands-on" and "hyper-involved" style). According to Plaintiff, CW4 and CW5 believed that St. Ledger's "team did not integrate well," and that St. Ledger and Rowland "'pushed out' all of the 'founding fathers' of Okta" in favor of hiring "people they had known from previous positions." (¶¶ 66–67.) CW5 also takes issue with changes that St. Ledger and Rowland made to the "customer segment structure," their management style, and the availability of revenue information. (¶ 90.) These are hindsight complaints about management, not evidence of securities fraud. *Dothill*, 2009 WL 734296, at *7 (finding no scienter based on "confidential witnesses [who] present only 'a litany of employee complaints about how [the company] was managed during the relevant period'"). None of these allegations demonstrate that St. Ledger and Rowland were aware that any of the challenged statements about the Auth0

integration were false or misleading. Plaintiffs, therefore, have failed to plead specific facts demonstrating that either of these non-defendants—who are not alleged to have made any challenged statement—possessed fraudulent intent.

Second, the knowledge of these two non-parties could not be imputed to Okta in any event because Plaintiff pleads no facts demonstrating that St. Ledger and Rowland had the authority to speak for Okta or control its statements. *See Alphabet*, 1 F.4th at 705 (scienter of "senior *controlling* officers may be attributed to the corporation itself" (emphasis added)).

***5. The Competing Inference Is Far More Compelling Than Plaintiff's Theory That Defendants Deliberately Misled Investors.***

To determine whether Plaintiffs have met their burden of pleading facts supporting a "strong inference" of scienter, the Court must not only consider "inferences urged by the plaintiff," but also engage in a "comparative evaluation" and consider "competing inferences [in defendants' favor] drawn from the facts alleged." *Tellabs*, 551 U.S. at 314. A complaint satisfies the scienter pleading requirement only if the specific factual allegations give rise to an inference of scienter that is "cogent and at least as compelling as any opposing inference of nonfraudulent intent." *Id.* Here, the non-fraudulent inference drawn from the allegations in the Complaint far outweighs any competing fraudulent inference.

As to the security incident, Defendants' actions "demonstrat[e] a pursuit of truth rather than reckless indifference to the truth." *Higginbotham v. Baxter Int'l, Inc.*, 495 F.3d 753, 758 (7th Cir. 2007). After Okta first "detected an attempt to compromise the account" of a third-party sub-processor, the issue was "investigated and contained." (¶ 106.) When hackers posted online a few screenshots taken during the incident, Okta was transparent about what it had learned about the incident and the worst case scenario based on the information known at the time: that "'approximately 2.5%' of Okta's customers" could "'*potentially* be[] impacted.'" (¶ 108 (emphasis added).) All told, "[t]his was a prudent course of action that weakens rather than strengthens an inference of scienter." *Horizon Asset Mgmt. Inc. v. H&R Block, Inc.*, 580 F.3d 755, 763 (8th Cir. 2009).

And as to the Auth0 integration, Okta reported on the progress of the Auth0 integration, noting throughout the relevant period that the sales integration would take time and there was work to do in

the challenging process of unifying sales teams from the two organizations. (¶¶ 74, 85, 120, 136, 151, 156, 162.) While "Defendants were initially optimistic about the integration of the [Auth0] and [Okta] sales force," they "later discovered that the integration did not proceed as smoothly as they had hoped." *Equinix*, 2012 WL 6044787, at *7. That is an unfortunate business development that sometimes occurs in significant corporate combinations—not securities fraud.

Finally, the Court must weigh the fact that no Individual Defendant is alleged to have had any motive to deceive investors. No Individual Defendant is alleged to have sold Okta shares at suspicious times. And no Individual Defendant is alleged to have personally benefitted from withholding information about the Auth0 integration or the security incident. The absence of personal motive to deceive strongly supports a non-fraudulent inference. *Prodanova v. H.C. Wainwright & Co., LLC*, 993 F.3d 1097, 1103 (9th Cir. 2021) (because "the complaint fails to plead a plausible motive for the allegedly fraudulent action, the plaintiff will face a substantial hurdle in establishing scienter").

* * *

Whether considered individually or holistically, Plaintiff's scienter allegations fall far short of satisfying the heightened standard for pleading scienter as to any Defendant. Plaintiff's claims should be dismissed on this independent ground.

### C. Plaintiff Fails to Plead Section 20(a) Claims Against the Individual Defendants

Section 20(a) makes certain control persons liable for a controlled person's violation of the federal securities laws. "To establish a cause of action under [Section 20(a)], a plaintiff must first prove a primary violation of underlying federal securities laws, such as Section 10(b) or Rule 10b-5, and then show that the defendant exercised actual power over the primary violator." *In re NVIDIA*, 768 F.3d at 1052. Because the Complaint fails to allege a primary violation of the federal securities laws, Plaintiff's Section 20(a) claim against the Individual Defendants necessarily fails as well.

## VI. CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court dismiss the Complaint.

Dated: December 1, 2022

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Brian M. Lutz*
Brian M. Lutz

*Attorneys for Defendants Okta, Inc., Todd McKinnon, Brett Tighe, and Frederic Kerrest*